UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,765	07/07/2003	**Paul C. Kocher**	2007003 / CRYP2C1P1US	8024

7590 08/09/2010

Patent Department
Macrovision Solutions Corporation
2830 De La Cruz Blvd.
Santa Clara, CA 95050

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	**PAPER NUMBER**
2437	
MAIL DATE	**DELIVERY MODE**
08/09/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/614,765	**Applicant(s)** KOCHER ET AL.
	Examiner JEFFREY D. POPHAM	**Art Unit** 2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 June 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-14,16-22,24 and 25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-14,16-22,24 and 25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 July 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *20100610*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Remarks

Claims 2-14, 16-22, and 24-25 are pending.

Response to Arguments

1. Applicant's arguments filed 6/10/2010 have been fully considered but they are not persuasive.

Applicant first argues that a copy of the cited reference “On Digital Optical Disk” from “Computer Technique Issue 10”, dated 12/31/2000 is provided with the response. However, the Examiner only sees the same Chinese publication with the English writing "China Academic Journal Electronic Publishing House". As the Examiner cannot read Chinese, the Examiner is unsure as to whether this is the corresponding document, since no where does the document say “On Digital Optical Disk”, “Computer Technique Issue 10”, or that it is dated 12/31/2000 in the English language. Confirmation as to whether this is the appropriate document is necessary since the Examiner cannot tell whether this is the appropriate document or not.

Applicant argues that the references do not teach that the program logic is a portion of the content. This is found in Kyle, just as Applicant points out that Kyle discusses "Including decryption code as part of the data package". This clearly shows the decryption code (program logic) being a portion of the data package (content). Applicant goes on to argue that “in Kyle, the executable instruction portion of the data package only operates on the single data item of the package. Kyle does not describe and cannot support a system that provides program logic being a portion of the content and loaded on a playback device that can interrogate the playback environment, authenticate a revocations list, provide a set of decryption keys for a plurality of versions of the content, and control playback of the entire content." However, Kyle discusses providing various types of instructions/code within the data package. Examples of such would be the entirety of or an upgrade to a video player, decryption code, decompression code, antivirus code, and format translation code. Clearly, at least some of this code controls playback of the entire content, as the code may include the player that will play the data, decrypt the data, decompress the data, virus check the data, and/or translate the data. However, these types of code are not the only instructions/code that can be provided in the data package of Kyle.

In fact, Kyle explicitly notes that "one skilled in the art will appreciate that the invention is applicable to other types of processing which may be desired following and/or incident to the transfer of data" (Column 10, lines 7-10). Therefore, Kyle contemplates other types of processing to be implemented within the instructions provided in the data package. This processing which is desired following the transfer of data clearly includes such processing as that provided in Benaloh and Nonaka (e.g. authenticating a revocations list, providing appropriate decryption keys, etc.), as such processing is required in order to properly access the data/content.

Applicant also argues that Benaloh does not teach verification logic that interrogates a playback environment to verify at least one of a playback device identity and a user identity, as now claimed. It is noted that this aspect is found in Nonaka, as described below in the rejections.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/10/2010 has been entered.

Information Disclosure Statement

3. The information disclosure statement filed 6/10/2010 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

This IDS cites a piece of NPL named “On Digital Optical Disk” from “Computer Technique Issue 10”, dated 12/31/2000, which cannot be found in the file. There is a document from "China Academic Journal Electronic Publishing House" that appears to have been published in October, 2000 (bottom of the page has what appears to be a date formatted [Chinese characters]/2000/10. As this publication is in Chinese, it cannot be understood to correlate to the cited NPL on the IDS, even if this is the appropriate document. Confirmation as to whether this is the appropriate document is requested, such that the information disclosure statement may be fully considered.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 2-11 and 21-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 2 is directed to “A storage medium containing content with protections against unauthorized copying". However, the definition of a storage medium includes this medium being a signal or carrier wave on which the content is stored. In order to be statutory, it must be clear that the content is stored on a non-transitory medium (e.g. CD or DVD). A simple fix would be to replace "storage medium" with "non-transitory storage medium".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which

> said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2-13, 16, and 19-22, and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benaloh (U.S. Patent 7,065,216) in view of Nonaka (U.S. Patent Application Publication 2002/0035492), Kyle (U.S. Patent 6,141,681), and Morito (U.S. Patent 6,782,190).

Regarding Claim 2,

> Benaloh discloses a storage medium containing content with protections against unauthorized copying, the storage medium comprising:
>
> Content that is encrypted by using broadcast encryption, whereby each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the content and each of a plurality of unauthorized playback devices does not have keys sufficient for decrypting the content (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);
>
> A plurality of versions for each of a plurality of portions of the content, wherein the versions for each portion are distinguished from each other, the versions are encrypted with different keys such that each of the authorized playback devices is capable of deciphering at least one, but not all, of the versions of each of the portions, the combination of the portions decipherable by a given player being usable to identify the player, logic being further configured to provide a correct set of decryption keys for decrypting

each of the versions decipherable by a given player, at least one decryption key of the set of decryption keys for decrypting a corresponding one of the versions decipherable by a given player (Column 9, line 61 to Column 11, line 12); and

Interface logic defining an interface usable to interact with a user and to control playback of the content (Figure 1; and Column 3, line 24 to Column 4, line 40);

But does not explicitly disclose a digital signature authenticating at least an identifier of the storage medium, a revocations list for identifying at least one revoked storage medium, program logic for an interpreter of a Turing complete language, the program logic adapted for execution on a playback device in order to play the content, the program logic configured for installation on the playback device, the program logic further configured for cryptographically authenticating the revocations list, the program logic further configured to perform a security check that interrogates a playback environment of the playback device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address.

Nonaka, however, discloses an identifier of the storage medium (Paragraphs 137, 144, and 230);

A revocations list for identifying at least one revoked storage medium (Paragraphs 232-234);

Content that is encrypted by using broadcast encryption, whereby each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the content and each of a plurality of revoked playback devices do not have keys sufficient for decrypting the content (Paragraphs 105, 130, and 223-234); and

Program logic further configured for cryptographically authenticating the revocations list (Paragraphs 223-234);

The program logic further configured to perform a security check that interrogates a playback environment of the playback device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address (Paragraphs 121, 184-187, 211, 230-231, and 299; ownership checks and revocation list checks using IDs, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the revocation methods of Nonaka into the content protection system of Benaloh in order to allow the system to revoke entities, such as devices and media, that are to be disallowed access to content, thereby providing better assurance that media and devices are proper before allowing content usage.

Kyle, however, discloses program logic for an interpreter of a Turing complete language, the program logic being a portion of content and adapted for execution on a playback device in order to play another portion of the same content, the program logic being loaded with the content on the playback device (Column 3, line 28 to Column 4, line 30; Column 4, line 47 to Column 5, line 14; Column 7, line 59 to Column 8, line 5; and Column 9, lines 19-29); and interface logic defining an interface usable to interact with a user and to control playback of the content by using the program logic (Column 4, lines 7-30; providing updates/upgrades or the entirety of a video player, for example, will include such interface logic in the program logic). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the content protection system of Benaloh as modified by Nonaka in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Morito, however, discloses a digital signature authenticating at least an identifier of the storage medium (Column 7, line 38 to Column 8, line 13; and Column 9, line 51 to Column 10, line 9). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature and authentication techniques of Morito into the content protection system of Benaloh as modified by Nonaka and Kyle in order to allow the system to verify that the medium is authentic via a signature of a medium ID and/or other information and to disallow usage of content stored on the medium when the disk is not authentic, wherein authenticity of the medium is provided by use of a public key cryptosystem such that only one entity can generate the signature, but any entity can verify the signature.

Regarding Claim 3,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 2, in addition, Benaloh discloses performing a plurality of security checks and permitting playback of the content provided that the plurality of security checks are successful (Column 7, lines 31-47; and Column 9, line 61 to Column 11, line 12); and Kyle discloses that the program logic is configured to perform a plurality of security checks and permit playback of the content provided that the plurality of security checks is successful

(Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 24; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 4,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 3, in addition, Kyle discloses that the program logic is configured to invoke at least one cryptographic operation supported by at least one of the authorized playback devices (Column 4, line 57 to Column 5, line 14).

Regarding Claim 5,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 3, in addition, Kyle discloses that the program logic is configured to perform at least one operation necessary for decryption of the content by at least one of the authorized playback devices (Column 4, line 57 to Column 5, line 14).

Regarding Claim 6,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 2, in addition, Kyle discloses that a subset of the authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and the medium further comprising program logic which, when executed by a device of each vulnerable model, is configured to mitigate the vulnerability affecting the vulnerable playback devices, and perform at least one operation necessary for the vulnerable playback device to decrypt the content (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 7,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 6, in addition, Kyle discloses that the program logic includes executable code for a Turing-complete virtual machine (Column 3, line 66 to Column 4, line 6; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 8,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 6, in addition, Benaloh discloses that the operation necessary to decrypt includes updating a cryptographic key contained in the playback device (Column 7, lines 31-47; and Column 9, line 61 to Column 11, line 12).

Regarding Claim 9,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 6, in addition, Kyle discloses that the program logic for mitigating includes native executable code configured to detect whether security of a vulnerable device has been compromised (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 10,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 6, in addition, Kyle discloses that the program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 11,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 6, in addition, Benaloh discloses that the player comprises firmware (Column 7, lines 48-53; and Column 11, lines 13-42); and Kyle discloses that the program logic for mitigating includes an upgrade to the player for correcting at least one vulnerability (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 19).

Regarding Claim 12,

Benaloh discloses a device for securely playing content, the content including a plurality of regions each having multiple versions thereof, the device comprising:

A media reader for use in reading data from a storage medium (Figure 1);

A nonvolatile memory containing a set of cryptographic player keys for use with a broadcast encryption system (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

A bulk decryption module for decrypting encrypted content from the storage medium (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

Select a version of each of the plurality of regions, thereby generating a set of selected versions (Column 9, line 61 to Column 11, line 12);

Provide a correct set of decryption keys for decrypting each of the selected versions, at least one decryption key of the set of decryption keys for decrypting a corresponding one of the versions (Column 9, line 61 to Column 11, line 12);

Decrypt the selected versions, whereby a combination of the versions selected in the course of playing content from the storage medium uniquely identifies the device (Column 9, line 61 to Column 11, line 12); and

At least one codec for decoding content (Column 3, line 65 to Column 4, line 6);

But does not explicitly disclose identifiers of revoked media, a Turing-complete interpreter for executing program logic, the program logic configured to install from the media reader, cryptographically authenticating identifiers of revoked media, verifying whether valid digital signatures contained on the storage medium authenticate the storage medium and verifying whether the storage medium is identified as revoked, or the program logic configured to interrogate a playback environment of the device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address.

Nonaka, however, discloses identifiers of revoked media, cryptographically authenticating identifiers of revoked media, and verifying whether the storage medium is identified as revoked in the nonvolatile memory (Paragraphs 105, 130, 137, 144, and 223-234);

The program logic configured to interrogate a playback environment of the device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address (Paragraphs 121, 184-187, 211, 230-231, and 299). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the revocation methods of Nonaka into the content protection system of Benaloh in order to allow the system to revoke entities, such as devices and media, that are to be disallowed access to content, thereby providing better assurance that media and devices are proper before allowing content usage.

Kyle, however, discloses a Turing-complete interpreter for executing program logic, the program logic being a portion of the content and configured to load with the content from the media reader, the program logic being adapted for execution on the device in order to play another portion of the same content on the device (Column 3 , line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; Column 7, line 59 to Column 8, line 5; and Column 9, lines 19-29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the content protection system of Benaloh as modified by Nonaka in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Morito, however, discloses verifying whether digital signatures contained on the storage medium authenticate the storage medium (Column 7, line 38 to Column 8, line 13; and Column 9, line 51 to Column 10, line 9). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to incorporate the signature and authentication techniques of Morito into the content protection system of Benaloh as modified by Nonaka and Kyle in order to allow the system to verify that the medium is authentic via a signature of a medium ID and/or other information and to disallow usage of content stored on the medium when the disk is not authentic, wherein authenticity of the medium is provided by use of a public key cryptosystem such that only one entity can generate the signature, but any entity can verify the signature.

Regarding Claim 13,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the device of claim 12, in addition, Kyle discloses that the interpreter is configured to obtain the program logic from the media reader for loading on the device (Column 3 , line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 16,

Benaloh discloses a method for playing encrypted content from a storage medium, the method comprising:

Retrieving at least one player key from a nonvolatile memory (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

Using the at least one player key with a broadcast encryption system (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

Using a result of the broadcast encryption system to decrypt at least a portion of the content (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

Selecting a variant from a plurality of variants for each of a plurality of portions of the content, wherein the media player device for decrypting the selected variant and the media player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each portion (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

Providing a correct set of decryption keys for decrypting each selected variant, at least one decryption key of the set of decryption keys for decrypting a corresponding one of the selected variants (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

Decrypting each selected variant by using the provided correct set of decryption keys (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12);

But does not explicitly disclose verifying a digital signature for authenticating the medium, reading program logic for a Turing-complete interpreted language from the medium, using an interpreter to execute the program logic wherein the interpreter performs operations specified in the program logic including installing from a media player device, use of identifiers of revoked media, or interrogating a playback environment of the device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address

Nonaka, however, discloses cryptographically authenticating identifiers of revoked media, verifying whether valid digital signatures contained on the medium authenticate the medium, and verifying whether the medium is identified as revoked in the nonvolatile memory (Paragraphs 105, 130, 137, 144, and 223-234);

Interrogating a playback environment of the device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address (Paragraphs 121, 184-187, 211, 230-231, and 299). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the revocation methods of Nonaka into the content protection system of Benaloh in order to allow the system to revoke entities, such as devices and media, that are to be disallowed access to content, thereby providing better assurance that media and devices are proper before allowing content usage.

Kyle, however, discloses reading program logic for a Turing-complete interpreted language from the medium, the program logic being a portion of the content, the program logic being adapted for execution on a media player device in order to play another portion of the same content on the media player device, using an interpreter to execute the program logic wherein the interpreter performs operations specified in the program logic (Column 3 , line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; Column 7, line 59 to Column 8, line 5; and Column 9, lines 19-29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the content protection system of Benaloh as modified by Nonaka in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Morito, however, discloses verifying a digital signature for authenticating the medium (Column 7, line 38 to Column 8, line 13; and Column 9, line 51 to Column 10, line 9). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature and authentication techniques of Morito into the content protection system of Benaloh as modified by Nonaka and Kyle in order to allow the system to verify that the medium is authentic via a signature of a medium ID and/or other information and to disallow usage of content stored on the medium when the disk is not authentic, wherein authenticity of the medium is provided by use of a public key cryptosystem such that only one entity can generate the signature, but any entity can verify the signature.

Regarding Claim 19,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the method of claim 16, in addition, Nonaka discloses accessing a media revocations list to determine whether the medium has been revoked (Paragraphs 105, 130, 137, 144, and 223-234).

Regarding Claim 20,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the device of claim 12, in addition, Benaloh discloses that the set of cryptographic player keys is unique to the player and the program logic is configured to select a unique set of versions by using the unique set of cryptographic player keys (Column 9, line 61 to Column 11, line 12).

Regarding Claim 21,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 3, in addition, Benaloh discloses that the program logic that is configured to perform a plurality of security checks generates a security check result, the security check result for embedding into content rendered by a playback device on which the security check is performed (Column 9, line 61 to Column 11, line 12).

Regarding Claim 22,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the medium of claim 2, in addition, Benaloh discloses that the program logic is adapted to perform at least one security check, the at least one security check to verify a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device (Column 7, lines 31-47; and Column 9, line 61 to Column 11, line 12).

Regarding Claim 24,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the device of claim 12, in addition, Nonaka discloses that the program logic being configured to forego decryption of the selected version if the program logic identifies the media as revoked (Paragraphs 232-234).

Regarding Claim 25,

Benaloh as modified by Nonaka, Kyle, and Morito discloses the method of claim 16, in addition, Benaloh discloses that the program logic is adapted to perform at least one security check of a playback device seeking to play the content, the at least one security check adapted to verify a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device, and to inhibit at least one of full quality playback or reduced quality playback if at least one security check fails (Column 7, lines 31-47; and Column 9, line 61 to Column 11, line 12).

6. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Benaloh in view of Nonaka, Kyle, and Morito, further in view of Sugahra (EP 0 668 695 A2).

Benaloh as modified by Nonaka, Kyle, and Morito does not explicitly disclose means for reducing during a rendering process an output quality of the content in dependence upon whether a security requirement specified by the storage medium for high quality output is met.

Sugahra, however, discloses means for reducing during a rendering process an output quality of the content in dependence upon whether a security requirement specified by the storage medium for high quality output is met (Column 9, line 50 to Column 12, line 4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data quality altering system of Sugahra into the content protection system of Benaloh as modified by Nonaka, Kyle, and Morito in order to allow the device to alter the content that is displayed based on numerous factors, including country, rating, viewer's age, device's and medium's protection levels, and the like, thereby allowing a single piece of content to be viewed in many different forms dependent upon the above.

7. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Benaloh in view of Nonaka, Kyle, and Morito, further in view of Foote (U.S. Patent 6,164,853).

Benaloh as modified by Nonaka, Kyle, and Morito discloses the method of claim 16, in addition, Kyle discloses that the interpreter performs operations specified in the program logic to respond to selections from a user (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5); but does not explicitly disclose that the user selections include button presses on a remote control.

Foote, however, discloses that the user selections including button presses on a remote control (Column 1, lines 25-39). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the remote of Foote into the content protection system of Benaloh as modified by Nonaka, Kyle, and Morito in order to enable a user to operate the player from the comfort of a user's chair or sofa, thereby eliminating the need to physically interact with the player itself.

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Benaloh in view of Nonaka, Kyle, and Morito, further in view of Ford (Ford, Susan, "Advanced Encryption Standard (AES) Questions and Answers", 10/2/2000, pp. 1-5).

Benaloh as modified by Nonaka, Kyle, and Morito discloses the method of claim 16, in addition, Kyle discloses that the program logic directs the player to perform a cipher operation via the interpreter (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5); but does not explicitly disclose that the cipher operation is an AES cipher operation.

Ford, however, discloses that the cipher operation is an AES block cipher operation (Pages 1-5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption algorithm of Ford into the content protection system of Benaloh as modified by Nonaka, Kyle, and Morito in order to use an encryption algorithm that provides high security, performance, efficiency, ease of implementation, and flexibility and that is easy to defend against power and timing attacks.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437